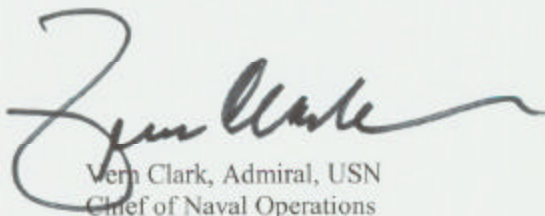




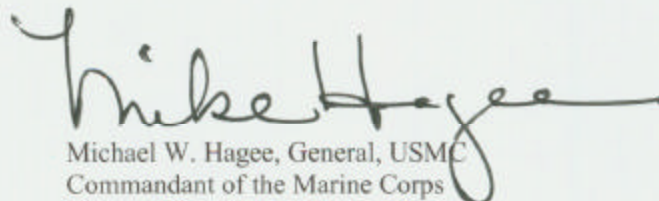
FORCEnet

A Functional Concept for the 21st Century

FORCEnet provides the naval command and control component for Sea Power 21 and Expeditionary Warfare, enhancing every aspect of naval, joint and combined operations. FORCEnet will empower Sailors and Marines at all levels to execute more effective decision-making at an increased tempo, which will result in improved combat effectiveness and mission accomplishment. As FORCEnet develops, it will fundamentally change the way the Navy-Marine Corps team functions by exploiting the power of networks—from deployed forces to the supporting establishment. A robustly networked Naval Force will improve situational awareness and mutual understanding, collaborative decision making, and operational planning by exploiting expertise resident throughout the force and beyond. This concept will yield better synchronization of actions through enhanced speed and quality of command. Although the focus of this concept is operational, FORCEnet is equally applicable to all activities throughout the Department of the Navy enterprise. This concept is derived from and further describes the vision of FORCEnet articulated in the Naval Operating Concept (2015-2020) for Joint Operations. It fully supports the Department of the Navy's Naval Power 21 and fundamental concepts and initiatives outlined in Sea Power 21 and Marine Corps Strategy 21. It aligns with evolving joint, interagency, and coalition command and control and net-centric concepts and capability-based guidance. This concept describes the principles, defines the capabilities, and reaffirms the necessity of co-evolving information technology with organization, process and doctrine. As such, this concept provides the overarching guidance necessary to support development of architectures, requirements, and future experimentation to fully realize FORCEnet. By doing so, the FORCEnet concept provides shared direction, guiding principles, and evolutionary objectives for the Navy and Marine Corps to develop future command and control capabilities.



Vern Clark, Admiral, USN
Chief of Naval Operations



Michael W. Hagee, General, USMC
Commandant of the Marine Corps

FORCEnet

A Functional Concept for the 21st Century

EXECUTIVE SUMMARY

This paper describes a concept for naval command and control for joint operations and supporting activities in 2015-2020 that will have dramatic and wide-ranging implications for the naval services. The intent is to establish a common direction for the diverse efforts that contribute to building naval command and control capabilities in the future and to provide a common framework for thinking about future command and control. The ultimate objective is to support the development of desired FORCEnet capabilities.

FORCEnet will serve as the primary catalyst for naval transformation; the result will revolutionize naval command and control. More broadly, FORCEnet has the potential to fundamentally transform operations themselves, generating higher tempo and greater effectiveness, efficiency and adaptability. Since force planning functions—such as training, administration, recruitment and acquisition—also require command and control, FORCEnet is expected to have the same transforming effect on the entire naval enterprise. FORCEnet is ultimately about fundamentally transforming naval operations and the entire naval enterprise.

FORCEnet is defined as the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force. The objective of FORCEnet is to provide commanders the means to make better, timelier decisions than they currently can and to see to the effective execution of those decisions. The underlying premise from which FORCEnet gets its power is the *network effect*, which causes the value of a product or service in a network to increase exponentially as the number of those using it increases. Since most headquarters are already well connected, the real power of FORCEnet is connecting the extremities of the force—individual people, weapons, sensors, platforms, munitions, shipments, end items, parts, and so on. A main objective of FORCEnet is extending visibility and empowerment to the extremities. The greatest breakthrough that FORCEnet will achieve in future command and control is in the area of maximum decentralization.

The fundamental hypothesis of this concept is that if all forces and organizations down to the level of individual entities are interconnected in a networked, collaborative command and control environment, then all operations and activities can enjoy the benefits of decentralization—initiative, adaptability and increased tempo—without sacrificing the coordination or unity of effort typically associated with centralization. This concept envisions command and control characterized by shorter decision cycles that allow commanders to make and implement better decisions faster than any enemy can tolerate. Based on improved situational awareness and mutual understanding throughout the force, commanders will more effectively impose their will on a situation and exercise initiative based on limited mission-type orders. At the same time, units and platforms will adapt more quickly and effectively to changing circumstances and self-synchronize their actions in furtherance of the mission.

As a system, FORCEnet constitutes the adaptive, distributed network of commanders, staffs, operating units, supporting organizations, sensors, weapons and other equipment interacting with one another on an underlying information infrastructure, as well as the associated command and control policies, concepts, organizations, techniques and procedures, standards and protocols, facilities and technologies, and supporting training and education that allow them to interact. As a process, FORCEnet constitutes an approach to commanding and controlling future forces based on the creation of network capabilities. The essence of this concept is a decentralized and highly adaptive form of command and control that uses the digital, global communication network to foster and exploit the human capacity for mutual understanding, implicit communication, and anticipatory cooperation. Exploiting the network effect achieved by organizing all nodes into an information-rich, collaborative, global network will enhance these qualities. Every node in the network—commander, staff, unit, supporting organization, platform, or piece of equipment—can be a producer, processor and user of information, and all information can be readily available to any node.

The command and control environment of 2015-2020 will pose significant challenges. Future enemies will employ new and unexpected methods developed to negate American superiority and exploit American vulnerabilities. Combat operations will likely be characterized by rapid and violent action in all dimensions simultaneously. Nonmilitary factors will be increasingly important in responding to crises, requiring better integration of military actions with the nonmilitary elements of national power. The U.S. military will likely be required to accomplish an ever-increasing range of missions creating an imperative for greater effectiveness and efficiency.

This document identifies the following capabilities as necessary to implement the FORCEnet concept.

- Provide robust, reliable communication to all nodes, based on the varying information requirements and capabilities of those nodes.
- Provide reliable, accurate and timely location, identity and status information on all friendly forces, units, activities and entities/individuals.
- Provide reliable, accurate and timely location, identification, tracking and engagement information on environmental, neutral and hostile elements, activities, events, sites, platforms, and individuals.
- Store, catalogue and retrieve all information produced by any node on the network in a comprehensive, standard repository so that the information is readily accessible to all nodes and compatible with the forms required by any nodes, within security restrictions.
- Process, sort, analyze, evaluate, and synthesize large amounts of disparate information while still providing direct access to raw data as required.
- Provide each decision maker the ability to depict situational information in a tailorable, user-defined, shareable, primarily visual representation.
- Provide distributed groups of decision makers the ability to cooperate in the performance of common command and control activities by means of a collaborative work environment.
- Automate certain lower-order command and control sub-processes and to use intelligent agents and automated decision aids to assist people in performing higher-order sub-processes, such as gaining situational awareness and devising concepts of operations.
- Provide information assurance.

- Function in multiple security domains and multiple security levels within a domain and manage access dynamically.
- Interoperate with command and control systems of very different type and level of sophistication.
- Allow individual nodes to function while temporarily disconnected from the network.
- Automatically and adaptively monitor and manage the functioning of the command and control system to ensure effective and efficient operation and to diagnose problems and make repairs as needed.
- Incorporate new capabilities into the system quickly without causing undue disruption to the performance of the system.
- Provide decision makers the ability to make and implement good decisions quickly under conditions of uncertainty, friction, time, pressure, and other stresses.

Fully realizing these capabilities will require developmental efforts across six dimensions:

- *Physical* -- the various platforms, weapons, sensors and other entities on the operating end of FORCEnet.
- *Information technology* -- the communications and network infrastructure through which these entities interact.
- *Data* -- the common structure and protocols for information handling.
- *Cognitive* -- human judgment and decision making and the human-computer interfaces that support them.
- *Organizational* -- the new force structures and working relationships that will be made possible by FORCEnet.
- *Operating* -- the emergent methods and concepts by which forces and other organizations will accomplish their missions due to the capabilities provided by FORCEnet.

The successful realization of FORCEnet will require a balanced approach that integrates all dimensions by combining doctrinal, organizational, training, materiel, leadership development, personnel and facilities initiatives.

FORCEnet

A Functional Concept for the 21st Century

INTRODUCTION

This paper describes a concept for naval command and control for joint operations and supporting activities in 2015-2020. The intent is to establish a common direction for the diverse efforts that contribute to building naval command and control capabilities in the future, and more broadly, to provide a common framework for thinking about future command and control. The ultimate objective is to support the development of desired FORCEnet capabilities.

This concept represents an early step in the capabilities development process. Many additional steps will be required to realize the envisioned capabilities. Informed by higher-level guidance, this concept provides direction for subsequent functional analyses, architectural design, force development recommendations, and implementation decisions such as those related to budgeting, acquisition and experimentation. This concept provides broad guidance in the form of a vision of future command and control. It prescribes no specific developmental solutions or processes because maturing FORCEnet capabilities will require significant judgment and creativity by all those involved in force planning.

The intention is that FORCEnet capabilities be fully realized by 2015-2020; individual capabilities will begin to appear before then. To reach this objective, all elements of force development—doctrine, organization, training, materiel, leader development, personnel and facilities—must begin moving toward that goal today. This paper identifies an initial set of capabilities required to implement this concept, and these provide a basis for developmental decisions.

This concept speaks primarily in terms of command and control of military operations, but the underlying principles apply equally to training, education, personnel and maintenance management, and all other supporting activities. FORCEnet applies to the entire naval enterprise.

This functional concept provides a strong emphasis on the power of Net-Centric Operations and the resulting increases in command and control effectiveness. It also provides insight into the associated risks of Net-Centric Operations and how to mitigate those risks. This document is not intended to encompass the full range of resourcing, acquisition, architecture, design and development of FORCEnet in the 2015-2020 timeframe. Follow-on concepts will expand on these areas.

IMPORTANCE of FORCEnet

FORCEnet has dramatic and wide-ranging implications for the naval services. It is intended to serve as an essential catalyst for naval transformation, revolutionizing naval command and control by 2015-2020. More broadly, because command and control naturally cuts across all military activities, integrating those activities and giving them direction, FORCEnet has the potential to transform operations by bringing about dramatically new and improved ways to operate. FORCEnet-supported operations are expected to have a higher tempo and greater

effectiveness, efficiency and adaptability. This means better results faster, with less waste and greater responsiveness to changing circumstances.

To an extent never before possible, FORCEnet will integrate people, weapons systems, sensors and other entities in a single command and control system—“connecting everything to everything.” A fully functional FORCEnet will empower commanders to integrate elements of the force they could not integrate before—or could not integrate quickly enough to make a difference.

Examples of practical enhancements expected from FORCEnet include improved combat identification to reduce fratricide, more responsive fires to attack fleeting targets, real-time tracking of logistics, and collaborative decision making that exploits expertise available anywhere in the world.

While it is true that this paper describes a concept for command and control, FORCEnet is not only about information systems or communications networks. It is ultimately about transforming naval operations.

ESSENCE of FORCEnet

FORCEnet is defined as “the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force.”¹

In simple terms, FORCEnet refers to the systems and processes for providing fully networked, naval command and control in 2015-2020. The objective of FORCEnet is to provide commanders the means to make better, timelier decisions than they currently can and to allow the effective execution of those decisions. The underlying premise from which FORCEnet gets its power is the *network effect*, which causes the value of a product or service in a network to increase exponentially as the number of those using it increases. The more units a weapon system can support, the more valuable is the weapon. The more decision-makers a sensor can provide with useful information, the more valuable is the sensor. The more commanders, staffs, units, platforms, weapons and sensors are linked together in a network structure, the more powerful will be the network. This concept envisions extensive connectivity among network elements—greater by orders of magnitude than previously achieved. Since most headquarters are already well connected, the real power in FORCEnet is in connecting the extremities of the force—people, weapons, sensors, platforms, munitions, shipments, parts, and so on. An objective of FORCEnet is extending visibility and empowerment of the extremities.² Network connectivity will provide all nodes, naval and non-naval alike, greater access to information, which will become the common property of the network.³

¹ Chief of Naval Operations, “FORCEnet Guidance,” Memorandum for Director, FORCEnet, undated. This basic definition was introduced by the CNO’s Strategic Studies Group.

² For an elaboration of this idea, see David S. Alberts & Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington: DoD Command and Control Research Program, 2003).

³ A node can consist of a single entity—a single instance of a physical thing such as an individual commander or other decision maker, a sensor, a weapon, a vehicle, a server, a supply pallet, or even a mechanical component or spare part—or a node may be a grouping of entities functioning as a single body—such as a staff, an analysis center, a combat unit, or an informal community of interest.

The hypothesis of this concept is that when all forces and organizations down to the level of individuals are interconnected in a networked, collaborative command and control environment, then all operations and activities will enjoy the benefits of decentralization—initiative, adaptability and increased tempo—without sacrificing the coordination or unity of effort associated with centralization. Most significant from an operational point of view, commanders will make and implement better decisions faster than any enemy can endure. Based on greater situational awareness and mutual understanding throughout the network, commanders will more effectively impose their will and exercise initiative in accordance with mission-type orders. At the same time, units and platforms will adapt quickly and effectively to changing circumstances and self-synchronize their actions in furtherance of the mission.

FORCEnet can be thought of as both a system and a process.⁴ As a system, FORCEnet is the adaptive, distributed network of commanders, staffs, operating units, supporting organizations, sensors, weapons and other equipment interacting in various ways on an information infrastructure, as well as the associated command and control policies, concepts, organizations, techniques, procedures, standards, protocols, facilities, technologies, training, and education that allow them to interact. It is important to understand FORCEnet as a system because developers will have to build that system. At its most basic, FORCEnet is a physical system consisting of people using information, supported by a networked command and control infrastructure.

FORCEnet also constitutes a functional process by which commanders recognize what needs to be done and ensure that actions are taken to accomplish the mission. The essence of this process is a decentralized, distributed and highly adaptive form of command and control that uses the digital, global communication network to broaden and exploit the human capacity for mutual understanding, communication, and anticipatory cooperation. Every node in the network—commander, staff, unit, supporting organization, platform, and piece of equipment—can be a producer, processor and user of information, and all information can be readily available to any node. Because of this connectivity command and control will be characterized by shorter decision cycles, enhanced shared situational awareness, and informed self-synchronization across the entire naval enterprise.

One of the most important things FORCEnet will achieve is to help commanders deal with uncertainty. FORCEnet should seek to reduce uncertainty to reasonable levels, but more importantly it should help commanders make effective and timely decisions in spite of uncertainty, because uncertainty is a fundamental attribute of all military operations. FORCEnet can do both by providing decision makers better access to any relevant information and providing better means for decision makers to visualize, share, and work with that information.

FORCEnet and COMMAND & CONTROL

Command and control is the means and methods by which a commander recognizes what needs to be done in any situation and sees that appropriate actions are taken.⁵ Command and

⁴ For more on command and control as a system and a process, see Thomas P. Coakley, *Command and Control for War and Peace* (Washington: National Defense University Press, 1992), p. 17. See also Naval Doctrine Publication (NDP) 6, *Naval Command and Control* (Washington: Department of the Navy, 1995), pp. 5-6, and Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control* (Washington: Department of the Navy, 1996), pp. 47-54. .

⁵ MCDP 6, p. 37.

control encompasses a wide range of activities, including: deliberative, creative decisions that devise concepts of operations; predetermined immediate-action drills; rules-based procedures for air-traffic control; automated fire control or combat direction, and many more. It ranges from the intuitive judgments that only skilled and experienced people can perform to the precise, instantaneous determinations that only automation can perform.

The Observation-Orientation-Decision-Action Cycle (or OODA loop) provides a fundamental model of the command and control process.⁶ The OODA loop captures the continuous and cyclical nature of command and control. The OODA loop will still apply in 2015-2020. FORCEnet, however, is expected to dramatically enhance the performance of the OODA loop, in three ways. First, it will accelerate command and control by changing the way information moves during the process, thereby speeding up individual phases of the decision cycle, collapsing phases into one another, and quickening the transition between phases. Second, it will facilitate a collaborative, team approach to the cycle, exploiting a division of labor and the distribution of expertise and understanding throughout the naval enterprise. Third, it will provide transparency to the command and control process, allowing for the spontaneous synchronization of multiple decision cycles across the enterprise.

FORCEnet views control as a state the entire system achieves based on feedback about the developing situation. Control is thus an emergent property of the organization arising out of the collective and transparent actions of the decision makers who exercise judgment and authority their own spheres while informed by a broader awareness. The goal is a process of continuous mutual influence in which commanding and controlling functions interact to ensure that the force can adapt quickly and effectively to changing circumstances. The quicker and more accurate the feedback, the more adaptive and effective the commander's decision making and direction.

Commanders and staffs, small unit leaders, individuals, and automated systems all perform command and control. Some forms of command and control deal with military science, while others involve the employment of military forces, through strategy, operations or tactics. Both are necessary, usually in some combination. The latter, however, is the highest form of command and control. It is at this level that leadership, the human component of command and control, has its fullest play.

FORCEnet must be able to support both centralized and decentralized command and control based on the requirements of each situation. That said, this concept generally envisions a highly decentralized form of command and control with respect to the overall conduct of operations. Despite advancements in technique and technology, there is a finite limit to the speed or attention of any one decision maker because there is a limit to the amount of information that any decision maker can use in a given period. The solution to this problem is to increase the number of decision makers while ensuring they work toward a common purpose. As a result, a key component of FORCEnet is empowering decision makers throughout the organization—out to the extremities—in order to increase both the speed and quality of decisions and actions. This emphasis on decentralization does not suggest that central authority is unimportant. However, the power of centralization is well understood, whereas the potential of connecting and empowering

⁶ Also known as the decision cycle or Boyd Cycle, after its creator, John R. Boyd. Boyd, "Patterns of Conflict" and "An Organic Design for Command and Control," *A Discourse on Winning and Losing*, unpublished briefing notes, 1987. Like any model, the OODA loop is naturally a simplification of complex reality. It is not meant to provide a complete description of the various phases and interactions, but rather a basic conceptual model. For a fuller description of the OODA Loop, see MCDP 6, pp. 63-65, and NDP 6, pp. 17-20.

the extremities remains largely unexplored. If FORCEnet achieves a true breakthrough in future command and control, it is likely to be in the area of maximum decentralization. In this context, the role of central authority is to provide a common direction for the various subordinate efforts ongoing, but in a way that does not unnecessarily constrain those efforts. Connecting the extremities can potentially generate tremendous capability, but without leadership from the center the decision makers at the extremities will lack the guidance that gives their decisions broader meaning. It is guidance from the center that unlocks the collective power of the full organization by allowing nodes at the extremities to act confidently with initiative.

FORCEnet and the HIERARCHY of MILITARY CONCEPTS

This functional concept for FORCEnet coexists with and is compatible with other existing future command and control functional concepts, such as the *Joint Command and Control Functional Concept*, the U.S. Air Force's concept for *Command and Control Constellation*, and the U.S. Army's *Battle Command* and LandWarNet. FORCEnet also encompasses the battlespace awareness and net-centric functions, which it considers subsets of command and control.

Functional concepts take their context from and must support higher-level concepts referred to as *institutional* and *operating* concepts. FORCEnet is compatible with and provides the command and control element in support of the higher-level concepts as described in *Naval Power 21*, *Sea Power 21*, *Naval Transformation Roadmap*, *Naval Operating Concept for Joint Operations*, and *Expeditionary Maneuver Warfare*. FORCEnet likewise provides the command and control element in support of subordinate concepts, or "pillars," of *Sea Power 21: Sea Strike*, *Sea Shield* and *Sea Basing*. Because FORCEnet will apply to every aspect of the naval enterprise, it also supports the Sea Warrior, Sea Enterprise and Sea Trial initiatives.

ASSUMPTIONS and RISKS

Two main assumptions about technological conditions in 2015-2020 form the basis for this FORCEnet concept:

- Information technology will continue to advance through 2015-2020 to an extent that can provide source information, connectivity and throughput that is sufficient and reliable enough to support the extensive communications envisioned by this concept.
- The Global Information Grid (GIG) envisioned in various joint and other future concepts will be a reality at some level and will include non-FORCEnet elements. This concept envisions that naval forces will be an integral part of a much larger joint, coalition, interagency and commercial network, that will enjoy magnified network effects because of its scope. Within the GIG, naval nodes will be inseparable from non-naval nodes. Naval nodes will rely on information and services provided by non-naval elements, just as they will contribute uniquely naval capabilities to the wider GIG.

Adopting FORCEnet carries with it certain risks. These include:

- Reliance on advanced information technologies inherent in this concept may make future naval command and control vulnerable to hostile information attack or exploitation.

- Reliance on advanced information technologies may also render future naval command and control less able to function effectively in the face of natural friction or any degradation.
- Information-management and processing technologies may not keep pace with rapidly increasing amounts of information, resulting in debilitating information overload.
- The expectation of large amounts of available information due to dramatic improvements in sensor capabilities may encourage a culture in which commanders are reluctant to act in the face of uncertainty.
- Extensive capabilities to exert command influence envisioned in this concept may encourage micromanagement by some commanders.
- Advanced information technology envisioned in FORCEnet may prompt decision makers to cede initiative to the intelligent systems they operate.

Developmental efforts—to include the full range of doctrinal, organizational, training, materiel, leader development, personnel, and facilities solutions—must strive to avoid or mitigate the effects of these and other risks.

COMMAND & CONTROL in 2015-2020

FORCEnet must accommodate likely changes in the future security environment that will affect command and control. Enemies will employ new and unexpected methods specifically developed to negate American superiority and exploit vulnerabilities. Future operations will be very complex. Nonmilitary factors will be increasingly important in responding to crises, requiring better integration of military actions with nonmilitary elements of national power. All of this will place increased strain on the ability to understand events and command and control.

The increasing range and lethality of weapons and sensors will expand the battlespace, as forces and platforms disperse for survivability. Many engagements will take place at greater distances, engaging the enemy from stand-off distances. A naval force could be required simultaneously to support operations in different operational areas or theaters. Enemies will target U.S. information systems as a cost-effective way of countering U.S. material advantage, so information assurance will be critical for effective command and control. The future will probably see decreases in U.S. overseas bases, which will mean decreased permanent command and control infrastructure. Potential operating areas in the developing world will be immature in terms of this infrastructure.

FORCEnet must support the full range of likely missions joint forces will be called on to perform. It must also support the operating concepts for performing these missions. Some aspects of operations will not have changed by 2015-2020. The naval roles of forward presence, deterrence and assurance, crisis response, and power projection will endure for the foreseeable future. U.S. forces must be prepared to participate in operations ranging from major combat on a theater level to noncombatant evacuations and other small-scale contingencies.

Future naval operating concepts envision naval forces organized into a greater number and variety of strike groups than currently—to include carrier strike groups, expeditionary strike groups, and surface action groups of various compositions.⁷ These naval and joint task forces will perform a wide range of offensive, defensive, and other operations from versatile afloat

⁷ Department of the Navy, *Naval Operating Concept for Joint Operations* (Washington: Department of the Navy, undated).

operating bases with minimal reliance on shore bases.⁸ These task forces are expected to exploit the mobility provided by command of the seas to maneuver directly and quickly against operational objectives in all dimensions—sea, land, air, undersea and space—in a form of naval maneuver warfare.⁹

FORCENet must support naval operations across the full width and depth of the joint battlespace: from the seabed to air and space, from deep blue waters to operational objectives ashore, from forward-deployed strike groups on the scene of a developing crisis to reach-back centers in the United States. FORCENet must support a wide range of types of military operations, including, but not limited to, small-unit urban operations, undersea warfare, theater air-and-missile defense, air-to-air combat, and special warfare.

Since all activities require command and control (broadly defined), FORCENet must support not only deployed operations, but also the day-to-day functioning of all supporting or shore establishments. Moreover, FORCENet will need to integrate the operations of deployed forces with these supporting functions because these latter ultimately exist only to support operations.

Despite dramatic improvements in information technologies, communications bandwidth will never be infinite, and throughput will sometimes be restricted due to hostile action, environmental conditions, or security requirements. This is especially true in certain domains, such as undersea, in which connectivity may be very limited and intermittent. Any future command and control system will therefore need to function satisfactorily under suboptimal conditions and be designed to degrade gracefully when required.

FORCENet will never reach a final state: there will always be a requirement to integrate “transformational” technologies, organizations and methods with “legacy” systems. This need for cross-generational integration will place a continual strain on command and control.

NETWORKING and SERVICES

The foundation upon which FORCENet is built is the communications network that provides interconnectivity among nodes, causing network effects to emerge. The FORCENet concept envisions largely unconstrained communications among nodes, unlimited by location, echelon or organization. Achieving this will require that all nodes adhere to common standards. This does not mean, however, that any node will routinely communicate directly with all other nodes. This highlights the importance of an intelligent information strategy to ensure efficient and effective management to guarantee that information is locatable, available and usable when and where needed. The objective is to optimize the flow of useful information while at the same time restricting the flow of unnecessary information—not a simple task, since the value of information changes from node to node.

Under this concept, all nodes become providers and users of services on the network. Services are any work performed by one node for another. These may be physical services, such as providing fires or logistics, or informational services, such as providing combat information or

⁸ Concepts known as Sea Strike, Sea Shield and Sea Basing. See Adm. Vern Clark, “*Sea Power 21: Projecting Decisive Joint Capabilities*,” Naval Institute *Proceedings*, October 2002.

⁹ United States Marine Corps, *Operational Maneuver From the Sea: A Concept for the Projection of Naval Power Ashore* (Washington: Headquarters U.S. Marine Corps, undated).

analysis or planning. In some cases, such as intelligence reporting, nodes will actually provide these services via the communications network, but in all cases they will transact these services by information exchange on the communications network. For example, a firing unit publishes to the network its availability to answer requests for fire, and a unit in contact subscribes to that service. Providers and consumers can likewise enter into service-level agreements, which are commitments among nodes to use and provide certain types and levels of service. Some services might be geographically limited, such as fires because of range limits, but many others will apply globally. The objective is an increasingly interdependent force. Units would no longer need the same level of organic capability because they will now rely on access to those capabilities as network services.

FORCEnet requires a service-oriented architecture based on several principles. First, any node can establish a presence on the network through which it can post the nature and location of its services and information. Second, others can easily find that node through accessible addressing. Third, others can then access the information and services they require, subject to necessary restrictions. Nodes will generally gain access to information and services by subscribing to them. In this way, decision makers choose, or “pull,” the information they need for their decision-making. This general “pull” approach should be balanced by intelligent “push,” whereby decision makers receive exceptional information they have not requested but which is deemed by some authority to be important to them. Commanders and staffs must use information push sparingly because excessive use can lead to information overload and to decision makers ignoring information, thereby missing the truly important information.

INTELLIGENCE, SURVEILLANCE and RECONNAISSANCE

The related activities of intelligence, surveillance and reconnaissance are key components of FORCEnet, supporting battlespace awareness—the *observation* and *orientation* phases of the command and control process. This concept envisions that intelligence, surveillance and reconnaissance activities will be provided as network services potentially available to any node, and capable of being integrated with other services at any level, rather than as organic capabilities dedicated to and optimized for one user only and capable of being integrated only at upper echelons.

This concept also envisions an increased emphasis on surveillance—on the persistent observation of extensive areas with a variety of redundant collectors. The objective is to provide continuous tracking of intelligence targets to anticipate and reveal patterns of activity. FORCEnet would routinely store the products from this surveillance to support after-action analysis of events—for example, tracing the origins of an enemy ambush or car bomb. This requires a varied array of technical sensors to achieve persistence, coverage, penetration, accuracy, responsiveness, and information retrieval. This requirement for technical sensors does not lessen the need for human intelligence collection, which must also have the timely means to post information to the network. Much intelligence information would be double-posted. Collectors would post time-sensitive combat information directly to the network for immediate exploitation by any node as appropriate. This same information would be picked up by analysis nodes, to enter the intelligence cycle and be re-posted as intelligence that has been processed, analyzed, evaluated and interpreted—while maintaining the correlation between the source data and the later intelligence product.

VISUALIZATION and COLLABORATION

With FORCEnet commanders and staffs, even when globally dispersed, will cooperate in a virtual work space to understand and represent a common problem and devise a solution to it. From a common, universal database they would be able create and share unique representations of the situation as it pertains to them. Since no two decision makers would have precisely the same perspective, there would be no effort to impose a single operating picture. Even when distributed globally decision makers would interact and cooperate, both vertically and horizontally, as if collocated. A plan would evolve out of the efforts of collaborative teams jointly creating a solution that belongs solely to no one decision maker, but is the collective product of multiple individual contributions.

FORCEnet will allow decision makers to collaborate implicitly as well as explicitly. Each user-defined visualization would exist in a shared space for others to see and use, providing the understanding that allows those others to cooperate with the decision maker without the need for direct communication or imposed coordination measures. Since decision makers need not even be aware that they are cooperating with one another, *implicit collaboration*—decision makers contributing jointly to a solution without any need for direct coordination—could result.

REQUIRED FORCEnet CAPABILITIES

This section describes the capabilities and attributes required to implement FORCEnet and how those capabilities fit together into the larger whole. The Navy and Marine Corps will develop some of these capabilities, while different organizations will develop others. Italics indicate capability attributes.

1. Provide *robust, reliable* communication to all nodes, based on the varying information requirements and capabilities of those nodes.

The foundation of FORCEnet is a *fully integrated, self-healing, self-organizing* communications system or infrastructure. This will consist of an interoperable worldwide network of information hardware and software and management services that produce and move information. It is this infrastructure that connects all nodes into an interactive system that generates network effects. It is this information network that will allow, for example, direct feeds from non-organic sensors to tactical commanders, the formation of virtual teams from among distributed elements, collaborative planning within these teams, and shared visual representations.

To optimize network effects, the infrastructure will be based on a *modular, open-systems architecture* which allow all nodes to interact regardless of location or network address. The network will include *accessible addressing* for all nodes, meaning that any node can efficiently locate any other node. The objective of this infrastructure is to communicate all necessary information to any node in the network quickly and without interruption. This information infrastructure must be compatible with the requirements of the Global Information Grid. It must connect not only all naval operating forces, but must also integrate these with naval support activities, other Service elements, nonmilitary agencies, and coalition partners. It must have sufficient throughput to ensure rich information sharing. It must be *robust* in that it will function in a variety of environments and *reliable* in that it must ensure that communication continues consistently under degraded operating conditions, including hostile attack of friendly information systems.

This capability will include a combination of permanent information infrastructure and expeditionary capabilities that exploit the full range of transmission technologies (radio, infrared, microwave, fiber, cable, etc.) and communications modes (voice, text, graphical, geo-spatial, etc.). Connectivity provided by this capability will be key to the organizational aspects of the concept—task-organized virtual teams and the spontaneous formation of communities of interest, by which necessary expertise is brought to bear regardless of geography or organizational structure.

2. Provide *reliable, accurate and timely* location, identity and status information on all friendly forces, units, activities and entities/individuals.

Capability 2 refers to gathering information from self-reporting elements. Once the underlying information infrastructure exists, self-reporting elements will generate the information that will serve as the first step in gaining situational awareness. Friendly units, equipment and supplies will automatically provide a steady stream of location and status information in real time. The information will depend on the type of asset that is reporting, and might include location, logistical or personnel status, operational readiness, current activity or mission, disposition, and plans. Weapon systems could report location, speed, azimuth, area of coverage, on-board ammunition supply, engagement criteria, or current activity. Automation should aggregate entity-level information to provide unit-level summaries at any echelon desired.

The information must be *reliable, accurate and timely*. Reliability refers to producing information on a dependable basis—the standard being higher for friendly information. Every FORCEnet entity will know its precise location at any moment in time, and should know where other FORCEnet entities think it is. Accuracy refers to the correspondence of the information with reality. Timeliness refers to gathering information in a period of time within which it is still relevant to decision making.

3. Provide *reliable, accurate and timely* location, identification, tracking and engagement information on environmental, neutral and hostile elements, activities, events, sites, platforms, and individuals.

Capability 3 refers to gathering information on any elements that are not self-reporting—including meteorology, geography and oceanography. This concept envisions more comprehensive and higher-quality information available about the enemy than ever before, due to emerging advances in sensor technology that will pursue the aim of *continuous* and *pervasive* surveillance. The goal is not only to detect, locate, identify and target, but also to infer capabilities and intentions—although it is important to keep in mind that no amount of surveillance will ever provide complete understanding of enemy plans and intentions.

4. Store, catalogue and retrieve all information produced by any node on the network in a *comprehensive, standard* repository so that the information is readily *accessible* to all nodes and *compatible* with the forms required by any nodes, within security restrictions.

Once information has been collected or created, it must be stored so that it is available for use when needed. Information collected or generated by any node will be captured and stored in shared space where it is available for use—that is, the data storage must be *comprehensive*. A shared space is a mechanism that provides storage of and access to data for uses within a bounded

network space.¹⁰ This applies to any form of information, including, for example, imagery, plans, graphics, position reports, battle damage assessments, logistical status, intelligence analysis, command guidance, and audio and text communications. It is not enough to store this information: it must be stored in a *structured* way that makes it readily *accessible* to any node with the necessary permissions. Making information accessible involves tagging information with metadata, which is information about the meaning of other information.¹¹ Metadata can describe or summarize key attributes of a piece of information to facilitate finding that information when needed. A key element of metadata is a time stamp that specifies when a piece of information is created.

Information storage must have *continuous* and *assured* access that is not subject to systemic shutdown. This shared space need not be a central database, but may itself be a distributed network with no single point of failure. When stored in the shared space, information must be *permanent*, meaning that it is safe from destruction, corruption or manipulation.

The format of information must be *standard*. All nodes must produce information in a format that is compatible with the network repository and all information in the repository must be in a format that can be recognized and retrieved by all nodes.

5. Process, sort, analyze, evaluate, and synthesize large amounts of disparate information while still providing direct access to raw data as required.

Once information has been made available in a shared space, it must be examined and processed to make it more valuable to decision makers. This information management generally should occur as a service provided on the network. Information carries a certain amount of value in itself, but it can become more valuable when formatted into a more useful form, combined or compared with other information, and analyzed and evaluated for meaning and implications. In this way, data are turned into knowledge and knowledge transforms into understanding. Information systems should be designed to provide commanders with higher levels of information rather than huge amounts of data, but without preventing commanders from directly and readily accessing key data elements as needed. In the collaborative environment envisioned in this concept, the aim should be to make it easy for others to add value to any piece of information.

Information management systems should be *flexible* in the sense that they allow the manipulation of information in a variety of different ways and combinations. All information should be *sortable* by any number of categories, including time, type and source. Much information processing and sorting can be automated. Automation can also assist humans in performing some higher-order functions, such as analysis, evaluation, and synthesis.

6. Provide each decision maker the ability to depict situational information in a tailorable, user-defined, shareable, primarily visual representation.

Working with information involves representing that information in ways that help commanders understand situations more intuitively and convey that understanding to others quickly and effectively. This is one of the most significant capabilities envisioned for

¹⁰ "DoD Net-Centric Data Strategy" (Washington: Department of Defense, May 9, 2003), p.8.

¹¹ Ibid., pp. 6-8. Metadata includes registries and catalogs. Registries contain information describing the structure, format, and definitions of data. Catalogs contain the actual metadata associated with a piece of information.

FORCEnet. Information should be representable in whatever form is most useful. This can include audio or text, but most often, it will be visual. This capability relies on the existence of comprehensive information storage and information management capabilities.

This capability assumes that all information that has been collected or created exists in a comprehensive repository and that some of that information has been processed, sorted, analyzed, and synthesized to give it more value to decision makers. Decision makers should be able to cut through this reservoir of data in any number of *flexible* ways, combining and recombining elements as desired to tailor a *user-defined* representation of the situation as it pertains to them. In an *intuitive* way, commanders should be able to cross-represent information by time, type, unit, size, activity, source, region, and so on, creating *tailorable* layers that can be turned on and off to reveal patterns and aberrations. These visualizations would represent not only the situation each decision maker faces, but also the intentions and plans for dealing with that situation.

Because these visualizations would all be networked, they would be *shareable* with all other nodes. This would allow each commander to gain insight into others' thinking, improving mutual understanding, and enabling commanders to self-synchronize with one another and mutually support one another with minimal need for explicit coordination. Because these visualizations are shared on the network, even though each node maintains its own visualization, commanders would be able to coordinate to reach common understanding and agreement about how to proceed.

Representations should be *polymorphic*—that is, the information should be capable of being represented in several different modes. The same information could be represented geospatially on a map, temporally on a time line, substantively as text or an image, graphically as part of a table or chart. This capability also implies the possible development of new visualization media, such as systems or influence diagrams to represent situational dynamics.

7. Provide *distributed* groups of decision makers the ability to cooperate in the performance of common command and control activities by means of a *collaborative* work environment.

Once information is represented, multiple decision makers must have the ability to work with it together on a common enterprise. The objective is that spatially dispersed decision makers collaborate with the same—or more—directness and richness of interaction as if they were collocated. With the ability to create user-defined visualizations, this represents potentially the most significant breakthrough capability of FORCEnet.

This concept uses the terms “collaborate” and “cooperate” synonymously, although the former implies intellectual effort and usually involves the creation of some product, such as a plan. The working together made possible by this capability could range from simple real-time coordination of some execution detail to sophisticated operations planning. The expectation is that decision makers would interact much more informally and would achieve greater mutual understanding.

Interconnectivity provided by networking makes this capability possible. Commanders are able to create virtual teams of any composition desired to collaborate on a mission. The collaboration would occur within the medium provided by the user-defined visualizations. Within this *primarily visual* work environment, decision makers would employ a suite of command tools, allowing them to create overlays, graphics, orders or other products. The tools in this environment should interface with other mission planning systems in a *seamlessly*

interoperable way. Plans would develop as collective efforts, with each team member contributing based on authority and ability. The plan would update in real time across the network as the cumulative effort of synchronous or asynchronous contributions.

8. Automate lower-order command and control sub-processes and to use intelligent agents and automated decision aids to assist people in performing higher-order sub-processes, such as gaining situational awareness and devising concepts of operations.

Some command and control activities must happen so quickly, routinely and consistently that machines best perform them. Other activities require the judgment and creativity that only experienced and trained people can bring. Automation can support both. Intelligently applied, it should result in higher-*quality* decisions made more *quickly* in both cases. In the case of lower-level functions, automation should perform those functions with greater *speed* and *accuracy* than people could. Even in cases in which people rely primarily on intuition, automation may assist with mechanical aspects of the activity, allowing humans to concentrate on the higher-level parts of the process, facilitating faster decision-making. Automation wisely used should mean that a greater proportion of the organization could dedicate itself to working on the actual problem at hand rather than being consumed with administration and other overhead activities. A corollary is that automation should make it possible to perform effective command and control with *fewer people*.

FORCEnet will involve a complex combination of machine-to-machine, human-to-machine, and human-to-human interactions, which will have doctrinal implications. FORCEnet requires the ability to manage these interactions. Machines will require the ability to recognize when automated processes have reached a threshold requiring human intervention.

Intuitive decision-making is a combination of the ability to recognize patterns and to simulate mentally the outcomes of possible courses of action.¹² Intelligent agents could potentially assist in both these areas. Significantly, simulations could be used to help commanders envision possible outcomes as well as anticipate unintended consequences, second- and third-order effects and possible enemy responses in complex situations.

9. Provide information assurance.

Protecting and defending information and information systems is a vital part of FORCEnet.¹³ It includes proactive and reactive computer network defenses organized as a *layered* defense-in-depth.¹⁴ Adversaries are likely to conduct a variety of sophisticated and unsophisticated information operations aimed at degrading or exploiting friendly command and control. Such operations could be a very cost-effective way to undermine U.S. operations. FORCEnet must therefore include the capability to protect command and control activities against efforts to deceive, exploit or otherwise attack them. This capability should include the abilities to detect, locate, and identify hostile information operations, defeat or counter those efforts, and mitigate the effects of successful hostile efforts. Information assurance also applies

¹² Gary Klein, *Sources of Power: How People Make Decisions* (Cambridge, MA: MIT Press, 1998), pp. 31-71 and 289.

¹³ Joint Pub 1-02: “**information assurance**—(DOD) Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation..”

¹⁴ Joint Pub 1-02: “**computer network defense**—(DOD) Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called CND.”

to accidental corruption of information. It should include the ability to recover to an earlier information state from any kind of information corruption.

This protection capability should be largely *automatic* and *autonomous*. It should routinely report hostile efforts according to conditions set by users, automatically handle those efforts within its means, and alert commanders to threats beyond its means. This capability should be *adaptive* and *learning*, meaning that it should adjust in response to changes in the conduct of hostile information operations.

10. Function in multiple security domains and multiple security levels within a domain, and manage access dynamically.

The logic of the network effect argues for few security restrictions because information generally is more valuable the more nodes have access to it. That said, protecting intelligence sources remains a valid concern and for that reason FORCEnet must include the ability to control access to information through the use of permissions. As a result, FORCEnet holds potentially significant implications for security classification. As a principle, information should be withheld only by exception rather than shared only by exception.

This capability requires keeping track of the classification of all information and the clearance of all nodes, and reconciling the two in an environment in which information is continuously moving through the communications network in numerous directions at once. The fact that collaboration will take place in groups consisting of changing joint, coalition and interagency membership with varying security clearances will complicate this. This concept envisions that information will routinely be sanitized or downgraded to lower security classifications using information management services resident on the network.

11. Interoperate with command and control systems of very different type and level of sophistication.

Because most future operations will be joint, FORCEnet elements must be fully and routinely *interoperable* with the systems of other services, creating a seamlessly joint command and control system. Because operations will also often be coalition and interagency operations, FORCEnet must be able to interface with the systems of nonmilitary agencies and other nations' militaries. Often these systems will be less sophisticated than U.S. systems, although some elements may be more sophisticated than elements of U.S. systems. Nonmilitary and foreign systems will likely have very different standards and conventions, so FORCEnet requires the ability to translate automatically as needed. Because command and control systems are ultimately human systems, joint, interagency, and coalition operations will invariably involve varying degrees of cultural differences, including differences in language and doctrine.

12. Allow individual nodes to function while temporarily disconnected from the network.

Although the FORCEnet concept depends on intense, networked communications, individual nodes should also have the ability to function, at least temporarily, while disconnected from the network or with limited throughput. Bandwidth is a limited resource. Throughput will usually be constrained, whether due to environmental factors or hostile efforts, especially since many enemies are likely to emphasize attack against U.S. information systems. Some nodes may choose to disconnect from the network temporarily for security reasons. This capability has two aspects. The first is functioning based on periodic network communications, which has different

implications for information management and situational awareness. The second aspect is retaining the *self-contained* or *autonomic* ability to perform certain core functions that would otherwise be transacted as services on the network. The level of autonomy that a node should have is a function of how much autonomy is feasible and how often the node can expect to be disconnected from the network. Some nodes, such as submarines, can expect to operate with very limited connectivity, and therefore may contain a high level of autonomy. Others can expect good connectivity, and therefore may rely more heavily on network services.

13. Automatically and adaptively monitor and manage the functioning of the command and control system to ensure effective and efficient operation and to diagnose problems and make repairs as needed.

FORCEnet will require its own command and control system, by which decisions will be made about managing and optimizing the performance of the system. This command and control capability should be a *networked* function, occurring as transactions of information, products and services on the network and generally making use of the same principles and interfaces as the command and control applications it manages. Monitoring and managing system performance requires instrumenting the system and its individual nodes to provide reliable status information.

This capability should be *automatic* and *adaptive*, providing for the rapid and efficient reallocation of resources—bandwidth, services, communication links, equipment, memory, personnel—and reconfiguring of system parameters in response to latencies, damage, overload or congestion, environmental interference (such as weather or sun spots), and so on. *Automatic* here means that much of this function should occur without the need for human interventions. *Adaptive* means that system management is responsive to changes in its own performance.

This capability should provide FORCEnet with *resilience*, the ability to recover from or adjust to stress or damage. This is critical since many enemies are likely to employ offensive information operations as a primary means to counter U.S. material superiority. When under attack or otherwise damaged, FORCEnet should be characterized by *graceful degradation* rather than catastrophic failure.

Since FORCEnet will be an open system which interacts with nodes and systems external to itself, this capability requires the ability to interoperate with the trouble-shooting and command and control capabilities of other systems.

14. Incorporate new capabilities into the system *quickly* without causing undue disruption to the performance of the system.

FORCEnet will never reach a final state. It will continually evolve as new advancements appear. Technology is advancing at an accelerating rate, and FORCEnet must keep pace with industry standards. Maximizing the effectiveness of FORCEnet over time requires incorporating new capabilities—technological or other—without disrupting the system. The incorporation of new capabilities should be *rapid* and *orderly*, suggesting a *modular* structure, which minimizes the systemic repercussions of introducing a new element, other than a fully integrated structure that tightly couples all elements.

15. Provide decision makers the ability to make and implement *good* decisions quickly under conditions of uncertainty, friction, time, pressure, and other stresses.

The primary reason for FORCEnet is to provide decision makers the ability to make and implement good decisions quickly. This capability is treated separately because of its importance and significant implications for nonmaterial solutions, especially education and training. This capability has two attributes: the *quality* and the *timeliness* of the decision, both of which can be difficult to measure, especially in the case of higher-order human decisions. The parameters of both attributes can also vary greatly, depending on circumstances. For example, some decisions made in seconds may be too slow, while other decisions made in days may be precipitous. In conflict situations, it is not absolute speed of decision that matters, but speed relative to the enemy's decision cycle. The ability to make a decision quickly does not negate the ability to bide time when the situation calls for patience.

WAY AHEAD

To understand the scope of FORCEnet, it is useful to think of the six “dimensions” identified by the CNO's Strategic Studies Group (SSG).¹⁵ The *physical* dimension includes the various platforms, weapons, and sensors on the operating end of FORCEnet. This dimension constitutes the adaptive, distributed network of entities that interact with one another to accomplish their various missions. The *information technology* dimension includes the communications and network infrastructure, which provides information services and assurance, architecture and standards, dissimilar redundancy, modularity and reconfigurability. This dimension requires security and must operate with other services, agencies, and coalition partners. The *data* dimension refers to the information itself that moves through the communications network. FORCEnet requires a common structure and language for information handling that is compatible with joint requirements as embodied in the “DoD Net-Centric Data Strategy.” It also requires a joint-compatible system of data-mining tools. These first three dimensions are embodied primarily in technology; they have tended to be the easiest to understand and have therefore received the most emphasis.

The implications of the latter three dimensions are more difficult to see, but are equally important to the eventual realization of the FORCEnet vision. The *cognitive* dimension refers to human judgment and decision making and the human-computer interfaces that support them. It includes augmented-cognition systems and other tools that can range from visual displays to multi-sensory feedback systems. The cognitive dimension is critically important to the development of FORCEnet and has significant doctrinal, education and training implications in addition to technological ones.

The implications of the last two dimensions derive from the developmental outcomes of the other dimensions and their interactions with one another. The *organizational* dimension refers to the structures of units or teams and the working relationships among them. The expectation is that FORCEnet will make possible organizations and processes—of both the command and control system specifically and the force more generally—that are much more efficient, effective and flexible, although it is impossible to know with any certitude at this point what those organizations and processes will eventually be. Only experimentation and experience will discover them. The *operating* dimension refers to the broad methods by which forces

¹⁵ Chief of Naval Operations' Strategic Studies Group XXIII, *Global Maritime Fight: 2030 and Beyond*, Quick Report, pp. 41-43.

accomplish their various missions. As with organization, the expectation is that FORCEnet will create opportunities for revolutionizing military operations. The same expectation applies to the naval enterprise. Operators and other users will invent these new methods by employing FORCEnet capabilities to solve the problems they face. These methods will be embodied in future operating concepts, which will undergo experimentation and evaluation eventually to find their way into doctrine.

While development of the first three dimensions—physical, information technology and data—will result primarily from technology improvements along current trajectories, development of the latter three—cognitive, organizational and operating—will be more a matter of thoughtful innovation. The successful realization of FORCEnet will require a balanced approach that integrates all of the dimensions through some combination of doctrinal, organizational, training, materiel, leadership development, personnel and facilities initiatives.

The implications of FORCEnet for force planning are dramatic. Many technological requirements may be direct and immediately discernible. Other implications, such as for personnel management or leader development, are less direct and will be more difficult to understand—and may become clear only after other areas have evolved. Although technology solutions are often the most obvious—and FORCEnet clearly depends on advanced technologies—it should not be assumed that most of these capabilities will be built primarily through material solutions. It is important to take an integrated approach, which will allow developers to make tradeoffs among different options. Areas are all interconnected, and initiatives in one area will have implications in other areas. For example, a new technology system will require training, organizational, doctrinal and manpower changes. Conversely, marrying an innovative technology to existing methods and organizations will result in marginal improvements at best—and may even prove counterproductive—but will almost certainly fail to live up to expectations or potential. Technologies should co-evolve with the other elements of force development.

The process of developing FORCEnet capabilities must be an adaptive, evolutionary process rather than an engineered one. While an implementation plan clearly is required and while it may be possible to anticipate some of the broad features of FORCEnet, it is impossible to describe the final product in detail at the beginning of the development process. No system as complex and adaptive as FORCEnet can ever be engineered in this way. Such a complex system can only emerge when conditions are right. FORCEnet will succeed only by evolving over time, when the proper conditions are fostered. The critical first step will be to connect large numbers of nodes and services in an open network that provides maximum freedom of interaction. A publish-or-perish mechanism should be created, whereby all nodes are compelled to publish their services on the network or find themselves irrelevant because they cannot participate in significant operating or enterprise interactions. The second step is then to allow operators and other users to identify the services and develop the processes that best help them accomplish their missions.

The developmental process must be agile and adaptive, involving continuous experimentation and incremental development. In this environment, users will demand and employ services that provide value and will ignore those that do not, establishing market mechanisms that reinforce the most valuable services and eliminate the least valuable. The needs of users will thus dictate where to focus developmental efforts and investments. To provide the rapid and meaningful feedback needed to “control” this process, developers should be embedded with operators and other users, iterating quickly in response to user requirements that co-evolve with new capabilities being introduced.

CONCLUSION

The FORCEnet Functional Concept envisions a highly adaptive and decentralized form of command and control that is consistent with naval tradition and is based fundamentally on the unique logic of networks. Connected by a global digital network, every node will be a producer, processor and user of information and services, and any information and service could be readily available to all. “Control” will not be imposed on the organization by upper echelons, but will emerge out of the collective and transparent actions of all decision makers exercising judgment and authority within their own spheres, while informed by broader and deeper awareness and infused by an understanding of the intentions of their seniors.

This command and control will be available not only to operating forces, but to all supporting activities as well. It will integrate both into a cohesive and adaptive naval enterprise that enjoys the initiative, adaptability and increased tempo gained from decentralization without sacrificing the coordination or unity of effort associated with centralization.

FORCEnet will be far reaching, touching every aspect of the naval enterprise. Successful implementation requires that all members of the Navy-Marine Corps team understand and appreciate the implications of FORCEnet, and actively pursue realization of the vision described in this concept.

APPENDIX A: An Example of FORCEnet

This illustrative scenario describes the dynamics of future command and control as envisioned through FORCEnet. It is not meant to be definitive or comprehensive.

In a hostile theater of operations in the year 2017: A human intelligence source reports the presence of unexpected hostile activity in a populated area near a recently deployed U.S. unit. The source's headquarters publishes the report to the network shared space that is accessible to all network nodes. The system software electronically alerts a collection manager, based on pre-established criteria, that the enemy is moving weapons. She immediately seeks information from the standing, dynamic library of intelligence data, and then requests priority surveillance by air and space platforms, the availability of which she finds published on the network. Information gleaned from these resources enables her to vector a low-observable unmanned aerial vehicle (UAV), one of several available to provide targeting information. Again, system software allows the passing of this information to a number of other sensor acquisition systems whose sophisticated algorithms ensure tracking of the enemy weapons even if the UAV loses sight of them.

At this point, FORCEnet allows the near-automatic coordination and the self-synchronization of many activities. Several firing units, tracking the information flow, indicate their availability. Based on established attack criteria, an authorized coordination cell chooses fire over maneuver and designates one unit to fire the mission. The fire direction calculations take into account the locations of friendly and neutral elements in the vicinity—the former being automatically self-reported, while the latter are gathered through a combination of self-reporting and collection. The fired munition deploys its own sensor to provide battle damage assessment (BDA), which a software agent automatically correlates with the BDA reports from the UAV. Intelligent software gains human approval to notify public affairs and information operations organizations of the fire mission, which enables them to view the BDA directly to be ready to deal with any repercussions. The public affairs section notifies appropriate media outlets via the network with an immediate explanatory statement and imagery from the joint task force (JTF), preempting hostile information operations.

FORCEnet facilitates actions that in the past required considerable human time and effort, all potentially distracting to the commander and staff during critical periods. Examples include: firing systems that automatically report ammunition status thereby triggering a resupply request; software that automatically aggregates the totals for all reporting entities in the theater; and a joint logistics agency that tracks all Class V supplies within the theater or en route, noting expenditure rates and initiating air shipment from out-of-theater stocks. These various calculations and decisions take place on different time lines—from seconds or minutes to days or weeks—but remain synchronized with one another.

Meanwhile, the original spot report and its confirmation also enter the intelligence cycle, at which point a staff officer assisted by decision-support tools detects an anomaly. Uncertain of what this means he reaches out to an informal collection of various experts who have formed a community of interest on the subject. A cultural anthropologist from a major American university shares an insight that sheds new light on the situation. A retired foreign area officer (FAO) who served in the region contributes additional perceptions based on his experience. A senior Defense Intelligence Agency (DIA) analyst synthesizes the work of the anthropologist, the FAO, and others, and postulates the emergence of a new hostile tactical technique that may also signal a new enemy operational initiative. The analyst immediately publishes details of the new technique to all joint, coalition and private security forces and other agencies operating in the

theater. Stateside operating forces undergoing predeployment training subscribe to the same information and learn about the new technique immediately. The information likewise goes to lessons learned centers throughout the U.S. military and, within weeks, a war college instructor incorporates the lesson into his course of instruction. This ability to tap into distributed expertise allows friendly forces to fight differently and to adapt rapidly.

To confirm the meaning postulated by the DIA analyst, a Naval Reserve intelligence analysis cell supporting the JTF examines satellite imagery, available from an online data storage service, for changes and pushes the results forward. An array of additional mobile sensors—UAVs and manned aircraft—is vectored to conduct electro-optical/infrared (EO/IR) imaging of sites identified by satellite. Analysts download communications intercepts in search of information to support or contravene the initial interpretation.

The staff officer reports his findings to the commander, who sees the opportunity to “get inside” the enemy’s decision cycle and seize the initiative. He quickly directs the formation of a distributed operational planning team (OPT) to review the situation. The OPT includes members from all service components, coalition partners, and governmental and non-governmental agencies. Some nodes are standing members of the OPT. Others are sought out on the network because of special expertise, while still others see the posting for the OPT and offer their services, believing they have something to contribute.

The OPT quickly concludes that neither the original plan nor its branches or sequels will suffice for the new situation and commences replanning. A decision-support agent searches an historical database of past conflicts and identifies and presents two condensed studies with possible similar characteristics for the team’s consideration. Participants draw in additional support to assist in a collaborative estimate that cuts across staff functions. After further examination of available information the JTF commander, in distributed collaboration with key subordinate commanders and nonmilitary leaders, quickly outlines a new course of action in preliminary form.

The JTF commander shifts from the sea base to a forward location ashore, but remains involved in the collaborative planning through “on-the-move” communications means. The plan grows quickly as the dynamic, collective product of the various participants, each contributing based on level and area of authority and expertise. The staff alerts a red team under contract to the Department of Defense—task-organized with expertise on the region and the particular enemy and updated with the latest downloaded threat information—which immediately commences trying to determine how an enemy could best counter the developing joint plan. Simultaneously, other analysts repeatedly run a multi-agent-based simulation of the plan on a national high-performance computer with changing variables, and provide the results to the commander and staff. As new information appears and lessons are learned, the plan evolves and the staff revisits and modifies basic decisions. Subordinate commands exploit visibility into the developing plans of adjacent elements to identify and resolve coordination issues and potential points of friction early in the process. Revised operations plans evolve and are war-gamed, refined and rehearsed in a virtual environment at multiple echelons simultaneously, updating the plan in real time across the entire joint force.

As execution begins, comprehensive self-reporting provides detailed information on the friendly situation, while access to the constellation of sensors and sources likewise helps commanders interpret the hostile, neutral and environmental situations. Commanders and staffs, aided by powerful information-processing software, use visualization tools to depict the situation as it pertains to them, and the networked collaboration environment allows them to share and

calibrate their understanding with one another. From the highest echelons to the extremities of the JTF, units and systems self-synchronize—from maneuver battalions coordinating their operational movements to individual sensors and shooters forming fleeting engagement linkages.

APPENDIX B: FORCEnet and UNCERTAINTY

The solution to uncertainty is timely, relevant information, but the issue is not as simple as reducing uncertainty by gathering more information. Situational awareness is not a matter of gathering as much information as possible to paint as complete a picture as possible. Rather, it is more often a sense-making process based on a small number of critical cues, while the vast majority of information is unimportant, irrelevant, or even misleading.

Uncertainty arises not only because information is lacking, but more often because information is unreliable or indeterminate. Uncertainty and information exist at several levels. Uncertainty may exist over data, the lowest level of information. Data are raw signals or unanalyzed reports. Data are generally the least important level of information from a decision-making perspective. The second level of uncertainty is the level of knowledge, at which data are interpreted and evaluated, and inferences are drawn. Intelligence is a form of knowledge, as opposed to unevaluated combat information.¹⁶ Even if a commander has reasonable certainty about existing conditions, it is difficult, if not impossible, to know what to infer from those data. This is especially true when dealing with an enemy who will have an incentive to be inscrutable and deceptive. The third level of uncertainty is the level of understanding at which inferences are synthesized into diagnoses and explanations of events and into projections about the future. Even if a commander can make reasonable estimates about what the data mean, he will not be able to predict eventualities with certitude. Understanding is a function primarily of experience and judgment. It can be aided by technology, but it is fundamentally a human skill.

As information ascends the hierarchy a synthesis occurs. Numerous pieces of data combine into a body of knowledge. Bodies of knowledge distill into understanding. This is a necessary process since otherwise commanders would quickly be overwhelmed with the amount of data to consider. FORCEnet should help commanders get past the data level quickly and spend more time working at the level of knowledge and understanding. But while an information-processing capability is necessary so that commanders do not need to wade through seas of mostly unimportant data, commanders must not be isolated from the data level. They must have direct access to the raw data as needed because they often base their understanding on a few key pieces of information.

¹⁶ Joint Pub 1-02: “**combat information**—(DOD) Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. See also information.”

“**combat intelligence**—(DOD) That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations.”

APPENDIX C: Glossary of Terms

accessible addressing—A feature by which any node in a communications network can readily locate and communicate with any other node in that network.

combat information—(DOD) Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. See also information.

combat intelligence—(DOD) That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations

command—(DOD) 1. The authority that a commander in the Armed Forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual.

command and control system—(DOD) The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.

communications net—(DOD, NATO) An organization of stations capable of direct communications on a common channel or frequency.

communications network—(DOD) An organization of stations capable of intercommunications, but not necessarily on the same channel.

community of interest—The inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange. (DoD Net-Centric Data Strategy)

computer network attack—(DOD) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Electronic attack (EA) can be used against a computer, but it is not computer network attack (CNA). CNA relies on the data stream to execute the attack while EA relies on the electromagnetic spectrum.

computer network defense—(DOD) Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. Also called CND.

connectivity—(DOD) The ability to exchange information by electronic means.

connections – The communications channels that interconnect FORCEnet nodes. The connections unite the nodes into a network. In this context, an architecture is simply a representation of these nodes and connections. Compared to other organizational forms, networks are characterized by pervasive communications—that is, many node-to-node connections in many directions. Networks tend to offer multiple, redundant paths between nodes. As a contrasting example, limited numbers of mostly-vertical connections generally characterize bureaucracies.

control—(DOD) 1. Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. 2. In mapping, charting, and photogrammetry, a collective term for a system of marks or objects on the Earth or on a map or a photograph, whose positions or elevations (or both) have been or will be determined. 3. Physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. 4. An indicator governing the distribution and use of documents, information, or material. Such indicators are the subject of intelligence community agreement and are specifically defined in appropriate regulations. See also administrative control; operational control; tactical control.

data asset—Any entity that is composed of data or a service provided to access data from an application. (DoD Net-Centric Data Strategy)

end item—(DOD) A final combination of end products, component parts, and/or materials that is ready for its intended use, e.g., ship, tank, mobile machine shop, or aircraft.

force planning—(DOD) Planning associated with the creation and maintenance of military capabilities. It is primarily the responsibility of the Military Departments and Services and is conducted under the administrative control that runs from the Secretary of Defense to the Military Departments and Services.

information—(DOD) 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.

information assurance—(DOD) Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA.

information operations—(DOD) Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. See also defensive information operations; information; offensive information operations; operation.

intelligence—(DOD) 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

metadata—Descriptive information about the meaning of other data. (DoD Net-Centric Data Strategy)

mission—(DOD) 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.

network -- not limited to the technical meaning of a system of computers, terminals, and databases connected by communications lines, although this certainly is a structural element of FORCEnet. A network has two types of elements: nodes and connections.

node -- The term “node” refers to any unit, thing or person within a network that can contribute, modify or use information there. As used here, nodes include non-naval elements that use or contribute information to the network. A node can consist of a single entity—a single instance of a physical thing such as an individual commander or other decision maker, a sensor, a weapon, a vehicle, a server, a supply pallet, or even a mechanical component or spare part. Alternatively, a node may be a collective, a grouping of entities functioning as a single body, such as a staff, an analysis center, a combat unit, or an informal community of interest.

open architecture —A type of system design that allows for upgrading or modifying the system by replacing, adding or subtracting components without disruption to other components or the system.

responsibility—(DOD) 1. The obligation to carry forward an assigned task to a successful conclusion. With responsibility goes authority to direct and take the necessary action to ensure success. 2. The obligation for the proper custody, care, and safekeeping of property or funds entrusted to the possession or supervision of an individual. See also accountability.

shared space—A mechanism that provides storage of and access to data for uses within a bounded network space. (DoD Net-Centric Data Strategy)

web services—Self-describing, self-contained, modular units of software application logic that provide defined business functionality. (DoD Net-Centric Data Strategy)